

**Reframing Intelligence: Challenging The Cold War Intelligence
Doctrine in the Information Age**

Author

Coyne, John, Neal, Stuart, Bell, Peter

Published

2014

Journal Title

International Journal of Business and Commerce

Rights statement

© 2014 Asian Society of Business and Commerce Research. The attached file is reproduced here in accordance with the copyright policy of the publisher. Please refer to the journal's website for access to the definitive, published version.

Downloaded from

<http://hdl.handle.net/10072/64647>

Link to published version

<http://www.ijbcnet.com/3-5/IJBC-14-3510.pdf>

Griffith Research Online

<https://research-repository.griffith.edu.au>

Reframing Intelligence: Challenging The Cold War Intelligence Doctrine in the Information Age

Mr. John Coyne

Australian Federal Police
QUT Faculty of Law, School of Justice

Mr. Stuart Neal

Australian Federal Police

Dr Peter Bell

Senior Lecturer, QUT Faculty of Law,
School of Justice
Adjunct Fellow Griffith University
Centre for Excellence in Policing & Security (CEPS)
p6.bell@qut.edu.au

Abstract

A complex international environment, increased availability of information, simplified data management tools and interfaces, and antiquated intelligence theory has given rise to intelligence clients performing their own intelligence analysis. In the absence of a clear delineation between policy and intelligence roles and outputs, intelligence (the function and the profession) is struggling to define its purpose in the ever-expanding information age. A review of the literature suggests that there has been an over-emphasis on the study (and subsequent analysis) of historical intelligence failures, but in doing so, has neglected to consider the challenges confronting contemporary intelligence managers and practitioners. This paper examines the need for intelligence policy makers to question the prevailing intelligence doctrine and argues that a greater emphasis be placed on the need to address the challenges of the information age within the context of a rapidly evolving operational environment. This paper argues that it is time for intelligence professionals to challenge the many fundamental assumptions that form the basis of western intelligence policy and practice. The paper seeks to advance discussion surrounding the maximization of intelligence resources, within the decision making process of western intelligence and security organizations. This discussion does not seek to further the debate surrounding a universal definition of 'intelligence'; but moreover, it is concerned with examining the role of intelligence in contemporary decision making.

Key Words: intelligence, security, organizational decision making, information age, knowledge management

1. Introduction

For intelligence and national security professionals, the years of the Cold War were defined by the presence of a clear and discernible threat, which provided a level of analytical certainty. This enabled the intelligence profession to develop detailed warning indicators and long-term predictions (Davis, 2007 and

2009). This clarity also facilitated the development of extensive intelligence collection capabilities, with large budgets being the norm (Fingar, 2011). Intelligence doctrine was developed, recorded, tested and based on the extensive military experience obtained during World War II and the consistent perceived threat posed by Communism. During the post-World War II period, the intelligence profession was able to undertake its work with almost negligible external criticism or accountability. Faurer (1999) noted that the intelligence profession was afforded the luxury of hiding behind the 'green door' of secrecy.

With the end of the Cold War came increased accountability, decreased budgets and an uncertain intelligence landscape where the nature and source of threats had changed (Fingar, 2011). The very nature of national security was challenged by the increased significance of non-state actors and the absence of a clearly defined 'enemy'. Betts (2009) argued that underlying intelligence doctrine from across the 'five-eye international intelligence community' remained for the most part, unchanged by this dynamic operating environment. Caverty and Mauer, (2009) further noted that despite its ever-changing environment, the organizational structures and decision making mechanisms of intelligence and security organizations appear to have stagnated in the post-Cold War period.

The September 11, 2001 terrorist attacks (referred to as 9/11 from this point forward) highlighted the inadequacies of the cold war intelligence doctrine in understanding emerging threats of the post-modern information age. The 911 Commission Report (2004) criticized intelligence both; coordination (a failure to share); and methodologies (a failure of imagination and collation/evaluation). While a deliberate policy response has been developed to address these specific findings, little has been done to address the underlying challenge that these observations pose to the theoretical construct of intelligence.

To date, the role of the intelligence professional has changed little since the beginning of the Cold War (Gill, 2009), despite the rapidly evolving decision making context of the post-modern information age, which presents substantive intellectual challenges to the intelligence professional, and aligned policy makers, very little appears to have changed with regards to the analytical tradecraft at this time. One of the fundamental questions for the intelligence profession is to determine if its half century old intelligence doctrine, remains valid and reliable today.

The perceived dormancy of intelligence doctrine can be contrasted with the exponential expansion of information available to public sector decision makers since the mid 1990's. In addition, the informatics tools that are used to exploit this vast quantity of data have increased at the same time as their technical interfaces have been simplified. Within the information age, knowledge and ready access to it, has become the decision-maker's currency. This phenomenon of abundant and accessible knowledge has arguably displaced the unquestioned pre-eminence of intelligence in public sector decision making (Davenport and Prusak, 1998; Frissen, 1999).

This paper explores these observations, and in doing so, highlights the need for intelligence policy makers to question the prevailing intelligence doctrine in order to meet the challenges of the information age and the post 911 intelligence operating context.

2. Discussion

2.1 The History of Modern Intelligence Theory

For almost 50 years scholars within the field of intelligence studies have focused on the development of an all-encompassing intelligence theory and a universally accepted definition of intelligence, with little

success (Kahn, 2009). It should be noted that the development of a universally accepted definition of intelligence remains a contentious and widely debated topic (Gill, 2009). The academic discourses and the theoretical positions of its various intelligence schools have had important impacts on the definitional work on intelligence across many non-national security and military applications of intelligence.

One of the most contentious issues surrounding this definitional debate involves the inclusion of ‘*covert action*’ and ‘*collection*’ activities within a working definition of intelligence (Johnson, 2009). One approach, which proffers the American military model of intelligence, argues that intelligence can be ‘*anything from any source*’ that aids decision-making (Warner, 2009; pp. 16-17; and Treverton, 2002).

Opposition to this approach suggests that intelligence is a secret activity (Matey, 2005; Shulsky and Schmitt, 1993; and Lowenthal, 2003). The secrecy approach has gained wide acceptance as illustrated by the Australian Intelligence Community (AIC) which specifically describes intelligence as covertly obtained information (ONA, 2006; p. 3). The secrecy approach however, is undermined by the increased use of open source intelligence material which is readily available within the public domain (Matey, 2005; Liapopoulos, 2006; and Dupont, 2003). Dupont (2003) supports this position by arguing that within the American Intelligence Community; approximately 70-80 per cent of the data held by US intelligence agencies is unclassified, open source information. But more importantly, the secrecy position fails to acknowledge that intelligence collection is a single stage in the intelligence cycle (Hulnick, 2002). There can be little doubt that the reliable and accurate covert intelligence can be integral to high quality intelligence products, but without evaluation and analysis, it remains covertly collected information for which little context is available.

It could therefore be argued that the inclusion of covert intelligence in any definition of intelligence may obfuscate the key challenges of the definitional endeavour. In a practical definitional sense, covert collection relates to the collection of ‘*secret intelligence*’. In this context ‘*secret intelligence*’ relates to intelligence which cannot be collected without the application of tradecraft and/ or technology to collect information that would not otherwise be available. It is intelligence that is collected from human sources (HUMINT) or via the interception of communications (SIGINT) (Congram, et al, 2013).

2.2 Intelligence Studies

Johnson (2009) argues that until the end of the Cold War, intelligence studies were divided between two schools of thought. One approach referred to as the American tradition, focused on studies which examined the conceptual and organizational issues of national security intelligence (Matey, 2005). The other approach is described as being supportive or a much more open view on intelligence and intelligence failures that are representative of the 21st century. In both cases, the approaches have been deeply rooted in exploring intelligence in the past, rather than the present. It could also be argued that these studies have ignored the rapid changes which have occurred with respect to the nature and scope of intelligence work.

Post-Cold War intelligence studies have seen the emergence of two new approaches to intelligence theory and practice: intelligence failure and strategic surprise (see also Cavelti and Mauer, 2009; Davis, 2003; and Matey, 2005). Since the 9/11 attacks, a plethora of academic studies of intelligence failure have been undertaken (see also Cavelti and Mauer, 2009; Davis, 2003; and Matey, 2005). These studies have been further supported by the declassification of primary research material relating to the Cold War (Laqueur, 2009). In each case, the findings appear to be similar in that they focus on the existence of intelligence/information silos, limited imagination, poor contextual understanding; and the over use of

historical pattern analysis methods /techniques (Cavelty and Mauer, 2009; and Laqueur, 2009). Analysis and research of past events more often than not, fails to declare the bias that hindsight creates for researchers (Holland, 2007).

Intersecting with the increased examination of intelligence failure is the increased study of strategic surprise (Davis, 2003). Rather than examining events as failures, this approach explores the causes and impacts of strategic surprise. Through this approach the issue of client relationships and communication are included in the scope of study (Wirtz, 2009; and Laqueur, 2009). This body of research focuses on developing the capacity of intelligence to anticipate future risks and threats in a generic sense, rather than in a precise and predicative manner (Davis, 2003).

2.3 Alternative Theoretical Paradigms

Since its inception, intelligence studies (the field of study) has concerned itself with the development of theories, and discourse on the application of intelligence in the fields of national security and military operations (Kahn, 2009). The foundation of intelligence theory and practice has subsequently been dominated by the national security axiomatic paradigm (Sheptycki, 2009; pp. 166-168). This paradigm has been developed on the assumptions and discourse of international relations realism, which focuses on conflict and the use of power including military action (Lawson, 2003; 78-82).

This theoretical construct now appears to place the intelligence profession at an impasse, where arguments about security in the post-Cold War era, remain focused on international relations (Fore, 2008). This discourse is concerned with distinctions of realist and idealist positions, which consider a world dominated by sovereign states (Liaropoulous, 2006). Within this conceptualization, intelligence is considered in terms of its utility in state on state conflicts. It could be argued that the intelligence profession is yet to deal with the post 911 period, let alone the emergence of the post international campaign against terrorism.

As a result of this narrow historical focus, theories on intelligence have been underpinned by the international relations paradigm (Liaropoulous, 2006). As a result, the study of intelligence has been firmly contextualized as an adjunct to international relations research (Kahn, 2009). The axiomatic focus on international relations has prevented intelligence studies from adopting an academic genus which incorporates national security, military, law enforcement and business intelligence (Hoogenboom, 2006; pp. 373-378). But just as importantly, it has led to an over simplification and often unhelpful understanding of the operating context faced by contemporary intelligence professionals. The intelligence focus in this context is concerned with reducing surprise and increasing advantage in conflict; whether kinetic, economic or legal.

The human security paradigm argues that intelligence provides decision makers with alternatives to the application of power and military action (Lawson, 2003; 89-91). This alternative could possibly become increasingly important as non-state and networked threats to national security become increasingly the norm rather than outlier issues (Turville, 2005; and Cavelty and Mauer, 2009). This alternative paradigm provides the intelligence profession with a wider scope for theory development that is focused on reduction of uncertainty in decision making.

3. Contemporary Intelligence Organizations

The study of (contemporary) intelligence organizational structures and functions further complicates the challenge of developing a universal intelligence theory. These organizational structures and functions are products of policy responses to historical drivers as opposed to examples of best practice. These intelligence drivers have impacted heavily on intelligence doctrine and practice in intelligence agencies in the United Kingdom, Canada, the United States, Australia and New Zealand (Liaropoulous, 2006).

The term '*intelligence community*' obfuscates the reality of contemporary intelligence organizations that appear to be individual stove piped components of a '*loose*' hierarchical organizational structure (Omand, 2010). The origins of the '*intelligence community*' concept can be found in the US response to intelligence failure following the Japanese attack on Pearl Harbour (Johnson, 2009). This failure lead the US President (at the time) to develop a 'bolt on' solution to the problem of intelligence stove piping, by creating a central intelligence agency to coordinate intelligence activities (Johnson, 2009). Within the United Kingdom, Canada, the United States, Australia and New Zealand, intelligence agencies continue to be divided by collection methodologies and function (Hastedt and Skelly, 2009; pp. 112-116).

The development of an intelligence definition and intelligence theory based on the '*intelligence community*' construct is thus impacted by the development of a structure that has more to do with political responses than optimum outcomes (Omand, 2010).

4. Access to Data

The internet, global connectedness, and the widespread distribution of classified government intranets did not exist in any substantive form until the late 20th century, and even then, not to a great extent compared to the present (Lowenthal, 2012). Until recently, intelligence clients were dependant on the information and intelligence assessments provided to them by their intelligence personnel. The information age has provided the individual with an ever expanding quantity and variety of information. The evolution of classified intelligence systems, including databases and applications (apps), has moved immediate access to holdings of raw information and intelligence product, from intelligence units/cells, directly to the decision maker's laptop. In addition, the front end interfaces, and backend information searching capabilities, have evolved to become more simplified and intuitive. This has arguably resulted in a more informed decision maker within intelligence organizations (Lowenthal, 2012).

Traditionally, intelligence staff and intelligence centers were not easily accessible. Intelligence capabilities, and their classified systems, operated behind locked doors (Faurer, 1999). As such, intelligence cells were the sole source of classified strategic and operational intelligence, information and local assessment. Intelligence cells defined themselves not just by their roles and products, but by what intelligence sources they alone had access to (Lowenthal, 2012). Behind these closed doors, analysts produced intelligence estimates, analysis, assessments, summaries, probes and intelligence reports. Intelligence personnel also operated as gatekeepers to other agencies' national, strategic, operational and tactical intelligence products and reporting (Davis, 2009). Until recently, decision makers had no other mechanism to access decision support material in a timely manner, than through intelligence cells (Lowenthal, 2012).

The information age has to some extent, reinforced the value of intelligence collectors and '*secret intelligence*'. In this context, secret intelligence refers to intelligence which is not available through open

source. But, intelligence theory has previously argued that intelligence is more than information sourced from secret sources. This gives rise to the question: *What does intelligence look like in the information age?*

During a recent intelligence analyst practitioner conference in Australasia, involving forty national law enforcement intelligence analysts, participants were asked: *'What products and services do you provide that no one else does?'* With thirty minutes having passed, the intelligence analysts were unable to identify or describe a specific skill set or service capability that was unique to their role description that could not be undertaken by other members of their organization.

The phenomenon of the information age has arguably displaced the unquestioned pre-eminence of intelligence in public sector decision making. In the post-modern information age, it has become far less clear to the policy maker or decision maker what intelligence is and what unique service or product it provides. The cold war era doctrine of intelligence theory is underpinned by a construction of the client as an entity unable to access or assess data and information. In this context, intelligence is at best, a classified information source. At worst the intelligence profession's analytical role is becoming redundant. Intelligence agencies' construction of the complexity of the national security environment has been characterised and driven by the nature of the Cold War. In this construct, world affairs have been dominated by the two to three major powers of the time. Subsequently, intelligence agencies' understanding of non-state actors, such as Al Qaida, was defined by their relationship to the major powers. This model could be legitimately sustained by analysts as the risk and threat posed by non-state actors was insignificant in comparison to the studied power blocs of the former Soviet Union and China (Powers, 2004). For example, the longevity of the Cold War, and the nature of both the conventional and nuclear war threat, meant that there would be lengthy periods of time before any large conflict could occur. Intelligence analysis was shaped by this situation. In the case of the former Soviet Union, US intelligence agencies were able to study Soviet military tactics and formations and develop response templates of their actions under various conditions. There was a high degree of confidence in these assessments due to the ability to rely upon years of in-depth analysis of a relatively static enemy (Powers, 2004).

It could be further argued that, the complexity of the international environment, the increased availability of information and data management tools, and historical intelligence theory have given rise to the concept of the client as an analyst. In the absence of a clear differentiation between policy and intelligence, analytical capabilities and roles, intelligence appears to be struggling to define its purpose in this post-modern information age.

4.1 Secret Intelligence

Intelligence customers increasingly value the receipt of raw secret intelligence, often at the cost of more detailed analytical products (Laqueur, 2009). Raw in this context refers to single source secret intelligence that has undergone limited analytical review and evaluation. Intelligence clients value these products as they provide privileged insights into another party's decision making process (Davis, 2009). But do intelligence clients that ingest such raw intelligence:

- Assess the veracity of reporting with an understanding of the limitations of technical collection capabilities?
- Consider the susceptibility of the reporting to deliberate deception?

- Methodically collate all source intelligence to thoroughly assess the validity and reliability of reporting?

From the clients' perspective, intelligence value is often reduced to the provision of '*Secret Intelligence*' and the insight it provides. But arguably, the role of the intelligence professional and the value provided is substantially more than the collection of secret intelligence. The collection of secret intelligence is a risky (high likelihood of compromise and high collateral consequences) and expensive activity (Laqueur, 2009). Two major contemporary sources of secret intelligence remain human (HUMINT) sources and communications intelligence (SIGINT) (Lowenthal, 2012, Congram, et al 2013). In both cases, the cost of maintaining collection capabilities is substantial, especially given the volume of national security issues now being considered. The information age continues to increase the cost and decrease the effectiveness of communications intelligence with the increased availability of '*off the shelf*' high-end encryption capabilities. Combined with growing public concern over the individual's right to privacy, the deployment of covert communication interception strategies by intelligence organisations and the subsequent use of intelligence derived from such strategies require careful ongoing consideration (Congram & Bell, 2010, Congram, et al, 2013, Bell & Congram, 2013a; 2014).

4.2 *The Policy-Intelligence Analyst*

Research of intelligence failures and strategic surprise has highlighted problems associated with the relationship and communication between intelligence and policy staff as well as decision-makers (Davis, 2003b). With the plethora of raw data, scholarly research and open source media reports available to decision-makers and policy staff, there is increasing evidence to suggest that many are undertaking their own research and analysis (Davis, 2003b). Davis (2003b) further argues that more often than not, such research is performed in a biased manner, where decision-makers and policy staff prefer research findings that support their own preconceived position on a particular issue. It could therefore be argued that the client of intelligence product has also become a competitor who is only further supported in their approach when intelligence fails to deliver innovative and convincing products. Davis (2007) specifically argues that intelligence professionals are experiencing increasing pressure to provide tailored reports that are consistent with the clients' analysis and preconceived position on a particular topic.

Following the analysis of intelligence failures, such as 9/11, there is considerable discussion within the literature regarding the relationship between the decision-maker and the intelligence professional (including the individual and the intelligence organisation) being 'too distant' (Davis, 2003b). Within the context of Iraq's Weapons of Mass Destruction, the issue of 'too close' a relationship between the two has been raised (Omand, 2010). It would appear that the issue is a paradox where the closer the relationship between policy and intelligence is evident, the greater likelihood of clear communication and support; however, as this relationship grows ever closer, there are forces that promote intelligence policy-product harmonisation (Davis, 2003b).

Holland (2007) argues that the value of national intelligence has now been called into question, given its spectacular failures with regards to predicting 9/11 and the existence of Iraq's Weapons of Mass Destruction. Combined, with the impact of the information age, and the findings from various inquiries into recent intelligence failures, it could be argued that the profession's relevance outside of informatics could be diminishing.

4.3 Evidence-Based Intelligence

In response to increased public scrutiny of national security and law enforcement organisations, the term ‘*evidence-based intelligence*’ has entered the lexicon of public commentators, law enforcement officers, policy staff and intelligence professionals (Mitchell, 2007; and Fingar, 2011). The term should not be misinterpreted to mean intelligence that is presented in a court of law, as evidence (Ratcliffe, 2008). This newer term relates to the level of confidence that a decision-maker can have in intelligence (Fingar, 2011). The term does not take into account the very nature of intelligence as ‘*value-added information*’ and may lead to intelligence being relegated to a knowledge management (KM) role (Lowenthal, 2012; and Laqueur, 2009).

Intelligence luminaries argue that intelligence is associated with the future and involves the intelligence professional analysing an incomplete data set (Fingar, 2011 and Sheptycki, 2009). By its very nature, future-based strategic intelligence could not meet any jurisdiction or commentators requirements for being ‘*evidence-based*’. This places intelligence professionals in a methodological paradox; to be ‘*evidence-based*’ it must await assessment to the evidentiary standard of ‘*beyond reasonable doubt*’, which makes it more akin to knowledge. By adopting this evidence-based approach, the timeliness of the intelligence could be affected and the value proposition of intelligence degraded.

Intelligence, which adequately identifies the future and communicates the decision priority accurately, should result in action (policy or strategy) (see also Caverty and Mauer, 2009; Davis, 2007 and 2009; Dupont, 2003; Lowenthal, 2012; and Fingar, 2011). It could be argued that strategy, if correctly developed, will have an impact and change the future state (Levi and Maguire, 2004). Thus, accurate intelligence will predict a future that will not occur because of strategic action. This gives rise to a complex paradox whereby intelligence that is increasingly accurate will eventually become increasingly inaccurate. This situation may inhibit the uptake of strategic intelligence given its perceived inaccuracies.

4.4 Informatics and KM

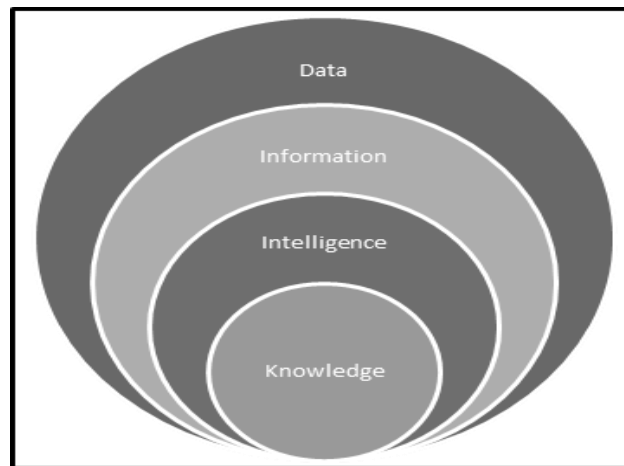
The field of informatics is concerned with the study of the natural and artificial systems which store, process, access, and communicate information (Dean & Gottschalk, 2007). It could be argued that intelligence is not a natural system that interacts with other artificial and natural systems. Whilst often involved or linked with information systems, intelligence is much more than the storage, processing, accessing and communicating of information. Within many western law enforcement agencies intelligence professionals have become increasingly involved and responsible for the organization’s information currency (Laqueur, 2009). More specifically, intelligence has become responsible for the processing and communication of information. It could be argued that this is not an intelligence function and that the transfer of this responsibility is based solely on administrative convenience and risk shifting as opposed to best practice.

Figure 1 provides a diagrammatical representation of the current conceptualization of data, information, intelligence and knowledge within the field of law enforcement (Dean and Gottschalk, 2007). Dean and Gottschalk (2007) provide a sound example of the degree to which the nature of law enforcement intelligence is misunderstood. Dean and Gottschalk (2007) reduce criminal intelligence to a simplistic formula: information plus organized analysis, equals intelligence. In part, this misnomer seems unsurprising when intelligence collection techniques (surveillance or human source for example) are so often mistaken for intelligence (see also Fingar, 2011; and Kahn, 2009). In adopting this approach intelligence in law enforcement is relegated to a position of data or crime analysis, without reference to its

predictive or anticipative value (Bell et al, 2010, Walsh, 2011). The model can be applied to a range of contemporary intelligence fields including military and national security applications.

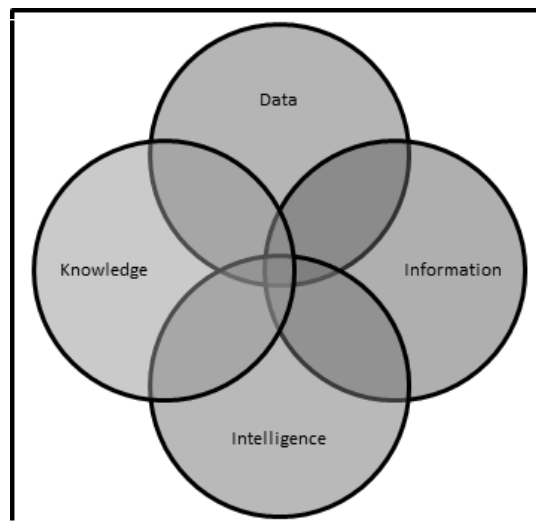
Figure 1 —Current Police Knowledge Management Continuum

(Source: Dean and Gottschalk, 2007)



The literature (Laqueur, 2009; Lowenthal, 2012; and Fingar, 2011), has consistently highlighted that intelligence is much more than information. As illustrated in Figure 2, intelligence may not sit within a data, information and KM continuum. Intelligence, within the context of this study, shares a number of common traits with data, information and knowledge (see Figure 2: Dean and Gottschalk, 2007).

Figure 2: Diagram of an Alternative Data, Information, Intelligence and Knowledge Continuum (Source: Dean and Gottschalk, 2007)



4.5 Future Focused Anticipative Intelligence

The theoretical construct of ‘*evidence-based intelligence*’ restricts intelligence to an information or KM paradigm of decision-support (Mitchell, 2007). Intelligence in this construct is, at best, relegated to the identification of the unseen, through detailed information analysis (Mitchell, 2007). Whilst there can be little doubt that these types of decision-support materials have untold value, they limit the application of ‘anticipative futures intelligence’ in problem solving (Quarmby, 2009; Lefebvre, 2010; and Liaropoulous, 2006).

Kahn, (2009) argues that a future-based theoretical framework for intelligence results in decision-support material with less analytical certainty than ‘*evidence-based*’ intelligence. As a result of the lower levels of analytical surety, intelligence products that identify risks and opportunities can be disseminated sooner than may have otherwise been possible in evidence-based constructs (Johnson, 2009). This future-focused intelligence support approach moves decision-making to a more proactive paradigm through the anticipation of developments (Quarmby, 2009). A recent case study of the Australian Federal Police revealed that strategic intelligence clients were often unable to clearly identify the impacts and strategic decisions arising from intelligence products (Coyne, 2014). Analysis of key strategic intelligence reports did not reveal what the implications of each assessment were for the reader or strategic decision-maker.

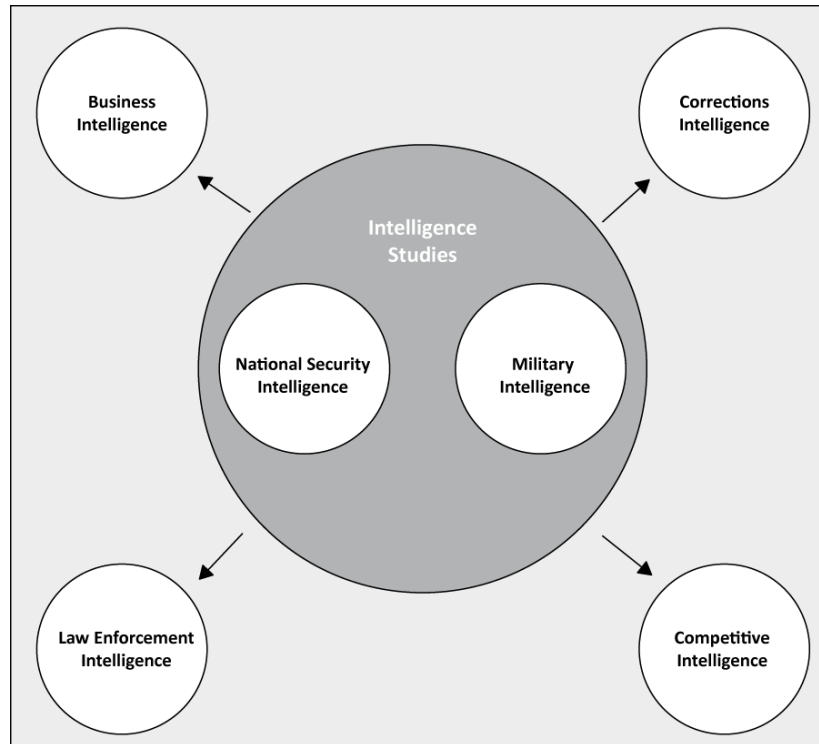
Contemporary intelligence theory argues that all intelligence reporting should provide an answer to the fundamental intelligence question of ‘*so what*’ (Fingar, 2011). The Australian Federal Police case study findings, implied that strategic intelligence in law enforcement may need to take this ‘*so what*’ process even further. In doing so, strategic intelligence should clearly articulate, and answer, the question ‘*so what does this analysis mean to the decision-maker*’ (Howlett, 2009). Intelligence theory for national security applications of strategic intelligence (Lowenthal, 2012) argues against such an endeavour. In comparison, Ratcliffe’s 3-I Model (2008) calls for the decision-maker to be presented with the answer to the question.

4.5 Reduction of Uncertainty

Figure 3 provides a diagrammatical representation of the overarching perceptions of intelligence theory, as espoused within the literature from the field of intelligence studies (Kahn, 2009; Davis, 2007; Lowenthal, 2012; Fingar, 2011; and Laqueur, 2009). Intelligence studies—born from the fields of military history, international relations and political science—serve as the source of contemporary intelligence literature and theory (Laqueur, 2009). As illustrated in Figure 3, intelligence studies remain focused on the application of intelligence within the national security and military spheres (Kahn, 2009; Davis, 2007; Lowenthal, 2012; Fingar, 2011; and Laqueur, 2009). Its theories are developed from a traditional international relations axiomatic paradigm that submits to the authority of the nation state (Sheptycki, 2009). These intelligence studies’ theories are then used within the wider intelligence context, such as law enforcement and business intelligence (Carter and Carter, 2009).

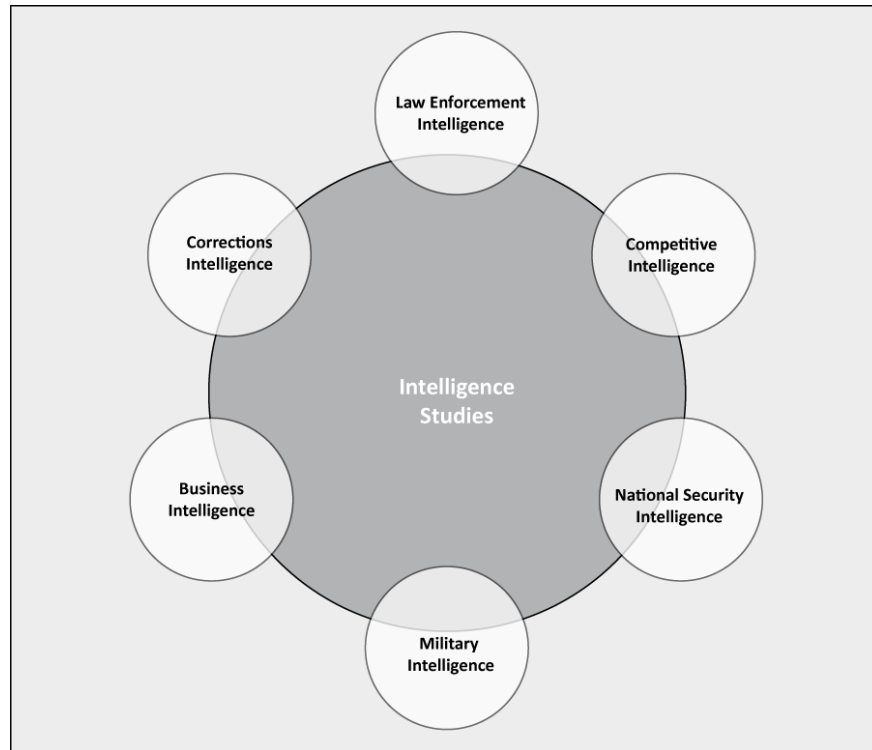
Figure 3 — Intelligence Studies' Conception of Intelligence

(Source: Kahn, 2009; Davis, 2007; Lowenthal, 2012; Fingar, 2011; and Laqueur, 2009)



The study of law enforcement intelligence has found that the separation of policy and intelligence may not be valid in law enforcement (Ratcliffe, 2008). The extrapolation of these findings indicates that the intelligence studies' focus on military and national security may not provide sufficient data to produce holistic theories across all applications of intelligence (Sheptycki, 2009). This observation questions the validity of the model in Figure 3. Figure 4 provides an alternative model for the conception of intelligence studies. Within this framework, intelligence studies are the genus, and the specific applications (business, competitive, corrections and law enforcement) are each part of the intelligence family. This hypothesis remains untested.

Figure 4 — Alternative Perception of the Field of Intelligence Studies



5. Future Research Directions

There can be little doubt the absence of a universal definition for intelligence continues to limit the development of intelligence theory. The differing perspectives of secret information, collection capabilities and analytical intelligence will need to be addressed before even the most general of definitions can be applied. In this context, there is a need for future research that seeks to compare and contrast the various applied definitions of intelligence (intelligence users, intelligence professionals, intelligence agencies and academia). This research should be focused on identifying the value proposition of intelligence for organizations. This research should also explore intelligence product differentiation from other organizational capabilities across defense, national security, and law enforcement environments.

Congressional commissions of inquiry into a number of recent intelligence failures have clearly identified 'collection imagination' as a 'significant contributing factor' in such events as 9/11 and the Iraq WMD failure (9/11 Commission Report, 2004) . The impact of these inquiries appears to have been limited given the methodological move away from the provision of predictive intelligence. There is an identified need for additional theoretical and applied research that examines the relationship between knowledge management, information and intelligence theory and practice. This body of theoretical research could form the epistemological basis for what intelligence does, through the development of a theory whose foundations are more fully understood.

While challenged to move beyond the limitations of data and information, the intelligence profession's ability to do so is being restricted by an increasingly complex operating environment and a growing risk

adverse clientele. The demand for analytical certainty, versus future orientated predictive or anticipative intelligence, requires further exploration so as to define its impact on the value proposition of intelligence for decision makers.

6. Conclusion

This article has sought to examine the challenges to the longevity of the intelligence profession. The professions adherence to an antiquated intelligence dogma has endangered its utility to clients. The distributed intelligence systems across the ‘five-eye communities’ have increased the importance of secret intelligence, but has simultaneously reduced the impact of analysis. The absence of the closed door organisational culture of intelligence has demystified the intelligence capability to such an extent that its relevance (in its current form) is in question.

While intelligence studies have been focused on axiomatic debates regarding a universal definition, clients have become their own analysts. Emerging research on data mining and data matching methodologies do little more than exacerbate the gap in understanding; intelligence collection, evaluation and e analysis. This presents intelligence practitioners, decision makers and scholars with an imposing research question; what does analysis provide the decision maker that they determine themselves. In many cases this has relegated the intelligence analyst to an information management or administrative role.

Now may be an appropriate time for the intelligence profession to re-examine and fundamentally challenge the underlying assumptions that underpin intelligence theory and practice. Through such critical analysis, the intelligence profession can more clearly articulate their value proposition to clients. The value proposition for an intelligence agency focused on the collection of secret intelligence is relatively easy, compared to intelligence agencies that support an analytical function.

For the intelligence practitioner, this paper reinforces the important role that client interface and direction plays within the process of the intelligence and the production of timely and accurate intelligence products. This is not to say that the customer is always right about what intelligence is, but ultimately, it is the client’s intelligence requirements that guide intelligence production. This highlights the need for intelligence professionals to move away from their traditional ‘output focus’ to a move ‘outcome focused’ model.

References

- I. Bell, P. and Congram, M. 2014, Communication interception technology (CIT) and its use in the fight against transnational organised crime (TOC) in Australia: A review of the literature, in the *International Journal of Social Science Research* Vol. (2), No. (1) pp. 46-66.
- II. Bell, P. & Congram, M. (2013a) Intelligence-led Policing (ILP) as a strategic planning resource in the fight against Transnational Organised Crime (TOC) in *the International Journal of Business and Commerce*, vol. (2), no. (12), pp. 15-28.
- III. Bell, P., Dean, G & Gottschalk, P. 2010, Information management in law enforcement: the case of police intelligence strategy implementation, in the *International Journal of Information Management*, vol. (30). no. (1), pp. 343-349.
- IV. Betts, R. 2009, 'Analysis War and Decision', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 87-112.
- V. Carter, D. and Carter, J. 2009, 'Intelligence-Led Policing: Conceptual and Functional Considerations for Public Policy', *Crime Justice Policy Review*, vol. 20, no. 1, April, pp. 310-325.
- VI. Caverty, M. and Mauer, V. 2009, 'Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence', *Security Dialogue*, vol. 40, no. 2, pp. 123-144.
- VII. Congram, M. & Bell, P. 2010, Laying the groundwork for the successful deployment of communication interception technology (CIT) in modern policing in the *International Journal for Policing, Intelligence and Counter Terrorism*, vol. (5), no. (1), pp. 9-27.
- VIII. Congram, M., Bell, P. & Lauchs, M. 2013, Policing Transnational Organised Crime, *Exploring the role of communication interception technology*, Palgrave MacMillan, Basingstoke, UK, pp.69-82.
- IX. Coyne, J. 2014, *Strategic Intelligence in Law Enforcement: Anticipating Transnational Organised Crime (TOC)*, unpublished doctoral thesis, Queensland University of Technology (QUT), Brisbane Queensland, Australia, pp. 88-89.
- X. Davenport, T.H. & Prusak, L. 1998, *Working Knowledge*, How organisations manage what they know, Harvard Business School Press, Boston, MA., pp. 27-29.
- XI. Davis, J. 2003, 'Strategic Warning: If Surprise is Inevitable, What Role for Analysis', *Occasional Papers: Sherman Kent Centre for Intelligence Analysis*, Vol. 2, No. 1, January, pp. 1-7.
- XII. Davis, J. 2003b, 'Tensions in Analyst-Policymaker Relations: Opinions, Facts and Evidence', *Occasional Papers: Sherman Kent Centre for Intelligence Analysis*, Vol. 2, No. 2, March, pp. 1-8.
- XIII. Davis, J. 2007, 'Intelligence Analysts and Policy Makers: Benefits and Dangers of Tensions in Relationships', in Johnson, L. (ed.) *Strategic Intelligence: The Intelligence Cycle*, Praeger Security International, New York, pp. 143-165.
- XIV. Davis, J. 2009, 'Strategic Warning: Intelligence support in a world of uncertainty and surprise', in Johnson, L. (ed.) *Handbook of Intelligence Studies*, Routledge, Taylor and Francis Group, New York, pp. 173-189.
- XV. Dean, G. and Gottschalk, P. 2007, *Knowledge Management in Policing and Law Enforcement: Foundations Structures, Applications*, Oxford University Press: London.
- XVI. Dupont, A. 2003, 'Intelligence for the Twenty-First Century', *Intelligence and National Security*, vol. 18, no. 4, August, pp. 15-39.

- XVII. Farson, S. 1989, 'Schools of thought: National perceptions of intelligence', *Conflict Quarterly*, vol. 9, no. 2, Spring, pp. 52-104.
- XVIII. Faurer, L. 1999 *Intelligence Support to the Warfighter, in Guideposts for the United States Military in the Twenty-first Century*, Air Force History and Museums Program, 16 September, Washington D.C.
- XIX. Fingar, T. 2011, *Reducing Uncertainty: Intelligence Analysis and National Security*, Stanford University Press, California.
- XX. Fore, H, 2008, 'Aligning "Soft" with "Hard" Power', *Parameters*, vol. 38, No.2, July, pp. 14-24.
- XXI. Frissen, P. 1999, A Post-modern Narrative on the Virtual State, in *Politics, Governance and Technology*, Edgar Elgar.
- XXII. Gill, P. 2009, 'Theories of Intelligence', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 208-226.
- XXIII. Hastedt, G. and Skelly, B. 2009, 'Intelligence in a Turbulent World', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 112-131.
- XXIV. Hoogenboom, B. 2006, 'Grey Intelligence', *Crime Law and Social Change*, vol. 45, no. 45, October, pp. 373-381.
- XXV. Howlett, M. 2009, 'Governance modes, policy regimes and operational plans: A multi-level nested model of policy instrument choice and policy design', *Policy Sciences*, vol. 42, no. 1, September, pp. 73-89.
- XXVI. Hulnick, A. 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Praeger, Westport, pp. 1-22.
- XXVII. Hulnick, A. 2002, 'The Downside of Open Source Intelligence', *International Journal of Intelligence and Counterintelligence*, vol. 15, no. 4, November, pp. 565-579.
- XXVIII. Johnson, L. 2009, 'Sketches for a Theory of Strategic Intelligence', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 33-53.
- XXIX. Kahn, D. 2009, 'An Historical Theory of Intelligence', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 4-15.
- XXX. Laqueur, W. 2009, *The Uses and Limits of Intelligence*, Transactions Publishers, London.
- XXXI. Lawson, S. 2003, *International Relations*, Polity Press, London.
- XXXII. Levi, M. and Maguire, M. 2004, 'Reducing and preventing organised crime: An evidence-based critique', *Crime, Law and Social Change*, vol. 41, no. 5, July, pp. 397-469.
- XXXIII. Liaropoulous, A. 2006, 'A Revolution in Intelligence Affairs? In search of a new paradigm', *Research Institute for European and American Studies Research Paper*, no. 100.
- XXXIV. Lowenthal, M. 2003, *Intelligence from Secrets to Police*, Washington D.C., Congressional Quarterly.
- XXXV. Lowenthal, M. 2012, *Intelligence: From Secrets to Policy*, Sage Press, London.
- XXXVI. Matey, M. 2005, 'Intelligence Studies at the Dawn of the 21st Century: New possibilities and resources for a recent topic in international relations', *UNESCI Discussion Papers*, no.8, May, pp. 1-15.

- XXXVII. Mitchell, M. 2007, 'Evidence-Based Policy and Proactive in Police Management', in Mitchell, M. and Casey, J. (eds.) *Police Leadership and Management*, the Federation Press, Sydney, pp. 75-89.
- XXXVIII. National Commission on Terrorist Attacks Upon the United States, 2004, 9/11 Commission Report, US Government, Washington D.C.
- XXXIX. Office of National Assessments, 2006, *The Australian Intelligence Community: Agencies, functions, accountability and oversight*, Office of National Assessments, Canberra.
- XL. Omand, D. 2010, 'Creating Intelligence Communities', *Public Policy and Administration*, vol. 25, no. 1, January, pp. 99-116.
- XLI. Powers, T. 2004, *Intelligence Wars, American secret history from Hitler to Al Qaeda*, New York Review Books, New York.
- XLII. Quarmbly, N. 2009, 'Futures work in Strategic Criminal Intelligence', in Ratcliffe, J. (ed.) *Strategic Thinking in Criminal Intelligence*, The Federation Press, Sydney, pp. 13-28.
- XLIII. Ratcliffe, J. 2008a, *Intelligence-Led Policing*, Willan Publishing, United Kingdom.
- XLIV. Sheptycki, J. 2009, 'Policing, Intelligence Theory and the New Human Security Paradigm', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 166-185.
- XLV. Shulsky, A. and Schmitt, G. 1993, *Silent Warfare*, Brassey's, Washington D.C..
- XLVI. Treverton, G. 2002, *Reshaping National Intelligence for an Age of Information*, Cambridge, Cambridge University Press.
- XLVII. Turbiville, G. 2005, 'Future Trends in Low Intensity Conflict', in Bunker, R. (ed.) *Networks, Terrorism and Global Insurgency*, Routledge, Taylor and Francis Group, New York, pp. 11-20.
- XLVIII. Walsh, P. 2011, *Intelligence and Intelligence Analysis*, Routledge Press, Sydney.
- XLIX. Warner, M. 2009, 'Intelligence as Risk Shifting', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 16-33.
- L. Wirtz, J. 2009, 'Theory of Surprise', in Gill, P. Marrin, S and Pythian, M. (ed.) *Intelligence Theory: Key questions and debates*, Routledge, Taylor and Francis Group, New York, pp. 73-87.